Security Evaluation of Online Signature Verification System using Webcams

T.Venkatesh
Research Scholar,
K.L.University,
A.P.,India

Balaji.S
Professor,
K.L.University,
A.P.,India.

Chakravarthy A S N
Professor,
K.L.University,
A.P.,India

ABSTRACT

This paper mainly focused on the evaluation of an authentication system based on personal signatures. Signature verification is an important research topic in the area of biometric authentication. In this paper the work is done in such a way that the signatures are captured using WEBCAM. A visual-based online signature verification system in which the signer's pen tip is tracked. The data acquisition of the system consists of only low-cost cameras (webcams) and does not need special equipment such as an electronic tablet. Online signature data is obtained from the images captured by the webcams by tracking the pen tip. The pen tip tracking is implemented by the Sequential Monte Carlo method in real time. Then the distance between the input signature data and reference signature data enrolled in advance is computed using Dynamic Time Warping (DTW). Finally, the input signature is classified as genuine or a forgery by comparing the distance with a threshold.

Keywords: Biometric Signature, Identification, Security, Verification

1. INTRODUCTION

Humans usually recognize each other based on their various characteristics since ages. We recognize others by their face when we meet them and by their voice as we speak to them. These characteristics are their identity. To achieve more reliable verification or identification we should use something that really recognizes the given person. The term "biometrics" is derived from the Greek words bio (life) and metric (to measure). Biometrics means the automatic identification of a person based on his/her physiological or behavioral characteristics. This method of verification is preferred over traditional methods involving passwords and PIN numbers for its accuracy and case sensitiveness. A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. These characteristics are measurable and unique. These characteristics should not be duplicable. An important issue in designing a practical system is to determine how an individual is identified. Depending on the context, a biometric system shown in Figure 1can either a verification (authentication) system or an identification system [1].

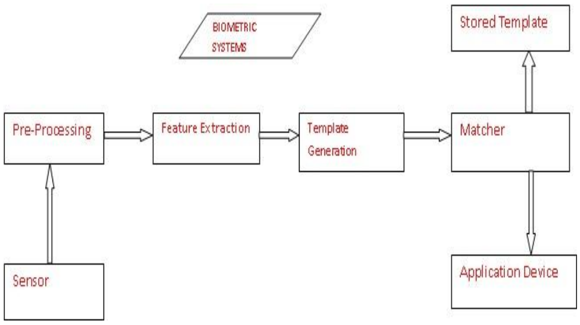

Figure 1: Biometrics Authentication system

1.1 Problem Statement

Signature verification techniques utilize many different characteristics of an individual's signature in order to identify that individual. The advantages of using such an authentication techniques are

(i) Signatures are widely accepted by society as a form of identification and verification.

(ii) Information required is not sensitive.

(iii) Forging of one's signature does not mean a long-life loss of that one's identity.

The basic idea is to investigate a signature verification technique which is not costly to develop, is reliable even if the individual is under different emotions, user friendly in terms of configuration, and robust against imposters. In signature verification application, the signatures are processed to extract features that are used for verification. There are two stages called enrollment and verification. In determining the performance of the verification system the selection of features takes main role and it is critical. The features are selected based on certain criterions. Mainly, the features have to be small enough to be stored in a smart card and do not require complex techniques. There are two types of features that validating a signature. They are static and dynamic features. Static features are those, which are extracted from signatures that are recorded as an image whereas dynamic features are extracted from signatures that are acquired in real time. The features are of two types, function based and parameter based features. The function based features describes a signature in terms of a time-function. Function based feature examples include position, pressure and velocity. Even though the performance of such features is accurate in verifying signatures, they are not suitable in this case due to the complexity of its matching algorithm. Hence, use of parameter based features is more appropriate. It is important to take into account external factors when investigating a signature verification technique. Nowadays signature verification applications are used in our daily lives and will be exposed to human emotions. The system has to give reliable accuracy in verifying an individual's signature even if user is under different emotions.

2. SIGNATURE VERIFICATION

Signature verification is a common behavioral biometric to identify human beings for purposes of verifying their identity. Signatures are particularly useful for identification of a particular person because each person's signature is highly unique, especially if the dynamic properties of the signature are considered in addition to the static features of the signature. Even if skilled forgers can accurately reproduce the shape of signatures, but it is unlikely that they can simultaneously reproduce the dynamic properties as well.

2.1 Types of Signature Verification

Signature verification is split into two according to the available data in the input.

A. Offline (Static): The input of offline signature verification system is the image of a signature and is useful in automatic verification of signatures found on bank checks and documents. Some examples of offline signature shown in Figure 2.

B. Online (Dynamic): Signatures that are captured by data acquisition devices like pressure-sensitive tablets (shown in Figure 3) and webcam that extract dynamic features of a signature in addition to its shape (static), and can be used in real time applications like credit card transactions, protection of small personal devices (e.g. PDA), authorization of computer users for accessing sensitive data or programs, and authentication of individuals for access to physical devices or buildings.

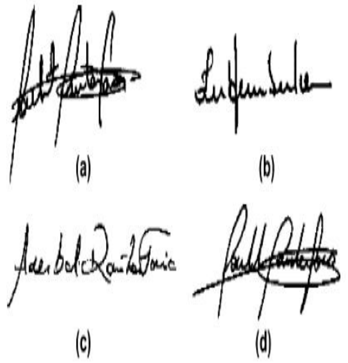

Figure 2. Offline Signature

Why Online (Dynamic)

Off-line signatures systems usually may have noise, because of scanning hardware or paper background, and contain less discriminative information since only the image of the signature is the input to the system. While genuine signatures of the same person may slightly change, the differences between a forgery and a genuine signatures may be difficult, which make automatic off-line signature verification be a very challenging pattern recognition problem. In addition, the difference in pen widths and unpredictable change in signature's aspect ratio are other difficulties of the problem

Figure 3: Online signature

It is worth to notice the fact that even professional forensic examiners perform at about 70% of correct signature classification rate (genuine or forgery).Unlike offline, On-line signatures are more unique and difficult to forge than their counterparts are, since in addition to the shape information, dynamic features like speed, pressure, and capture time of each point on the signature trajectory are available to be involved in the classification. As a result, on-line signature verification is more reliable than the off-line.

2.2 Performance Evaluation of Signature vs. System

For evaluating the performance of a signature verification system, there are two important factors: the false rejection rate (FRR) of genuine signatures and the false acceptance rate (FAR) of forgery signatures. As these two are inversely related, lowering one often results in increasing the other. The equal error rate (EER) which is the point where FAR equals FRR. There are two types of forgeries:

- A skilled forgery is signed by a person who has had practiced a genuine signature.
- A random or zero-effort forgery is signed without having any information and practice about the signature, or even the name, of the person whose signature is forged.

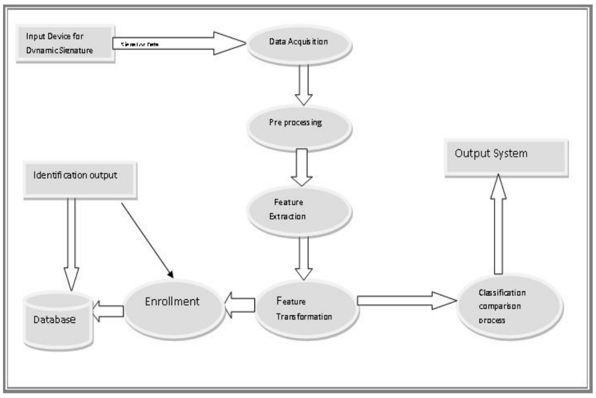

Figure 4: General System Overview

The performance of the available on-line signature verification algorithms give equal error rate between 1% and 10% , while off-line verification performance is still between 70% and 80% equal error rate. There have been several studies on on-line signature verification algorithms. On-line signature verification systems differ on various issues like data acquisition, preprocessing, and dissimilarity calculation.

2.3 New Extreme Points Warping Technique

Feng, in his paper [4] proposed a new warping technique for the functional base approach in signature verification. Dynamic time warping (DTW) is the commonly used warping technique. There are two common methodologies to verify signatures: the functional approach and the parametric approach so the functional based approach was originally used in application speech recognition and has been applied in the field of signature verification with some successful accuracy since two decades ago. The new warping technique he proposed, named as extreme points warping (EPW). It was proved that this method is adaptive in the field of signature verification than DTW in the presence of the forgeries. In the functional approach, a straightforward way to compare two signal functions is to use a linear correlation. It has the following two problems:

- ❖ Due to difference of overall signal duration.
- ❖ Due to existence of non-linear distortions within signals.

For a signal function, the signal duration is the same for different samples even from the same signer. In addition, distortions occur non-linearly within the signals for different signings. A non-linear warping process needs to be performed before comparison to correct the distortion. An established warping technique used in speech recognition is dynamic time warping (DTW). The use of DTW has also become a major technique in signature verification for the past two decades. Though DTW has been applied to the field with success, it has some drawbacks. DTW has two main drawbacks when applied in signature verification:

- ➢ It has heavy computational load,
- ➢ Another is warping of forgeries.

The first drawback is a known problem in case of speech recognition, because DTW performs nonlinear warping on the whole signal. For this method, the execution time is proportional to the square of the signal size; define boundary conditions in the DTW matching matrix to reduce the computation time. The second drawback, however, is not well documented in the past, but still got good accuracy and results as mentioned below in Table 2.4: A new warping technique called EPW replaced the commonly used DTW. Instead of warping the whole signal as DTW does, EPW warps a set of selective points.

We achieve the goal of warping the whole signal through matching the EPs and warping the segments linearly. Since EPW warps only EPs, the local curvatures between the EPs are saved, which prevents forged signals taking advantages from the warping process. Using EPW, the EER is improved by a factor of 1.3 over using DTW and the computation time is also reduced by a factor of 11. Hence this new technique EPW is quite promising to replace DTW to warp signals in the functional approach, as part of an effective signature verification system.

Table 1: new extreme points warping technique

Features used	Database sized				Features extracted	Results	
	Total persons	No. of sig/persons	forgers	Total/sign		ER (EPW)	EER (DTW)
*Rise Distance w.r.t time *Drop Distance w.r.t time	25	30	250	1000	Variation *Non-synchronicity for the start point *Existence of ripples *Non-synchronicity for the end point	27.9 %	35%

3. VISION SYSTEM FOR PEN TRACKING

In his paper Mario Enrique Munich [9], proposed the design of a system that captures both the spatial and temporal aspects of handwriting using a standard quality video camera as input device. Compare to others, cameras are of low cost and advances in manufacturing technology. There would be no need to buy additional hardware for the implementation of online signature verification system. We captured video while a subject writing on a piece of paper and we manually identified the position of the pen tip in each image of the sequence using a mouse. Author observe that the trajectories are a bit noisy especially the one tracked at 30hz.The pen tip position is collected for all the images of the sequence including frames both cases in which the pen is actually writing on the paper and frames in which the pen is travelling above the paper. After taking away the strokes that correspond to the pen moving above the paper and leaving only the strokes that correspond to the pen down on the paper. The trajectories are clear enough to enable one to easily read what was written.

3.1 System Description

Figure 4 shows the block diagram of the system and the experimental setup. The images captured by the camera are shown on the screen of the computer to provide visual feedback for the user. The user has the flexibility of placing the relative positions of the camera and the piece of paper in order to write with comfort as well as to provide the system with a clear sight of the pen tip. The camera captures a sequence of images to the preprocessing stage. This phase performs initialization of the algorithm, i.e., it finds the initial position of the pen and selects a template (rectangular sub region of the image) corresponding to the pen tip. In subsequent frames, the preprocessing stage has only the function of cutting a piece of image around the predicted position of the pen tip and feeding it to the next block. The task of pen tip tracker has to find the position of the pen tip in each frame of the sequence. The ballpoint detector finds the position of the very end of the tip, i.e., the place where the pen is in contact with the paper when the user is writing. The filter is a recursive estimator that predicts the position of the pen tip in the next frame based on an estimate of the current position, velocity and acceleration of the pen. The filter also estimates the most likely position of the pen tip for missing frames. At last, the last block of system checks the presence of ink on the paper at the ball point detected positions [10].

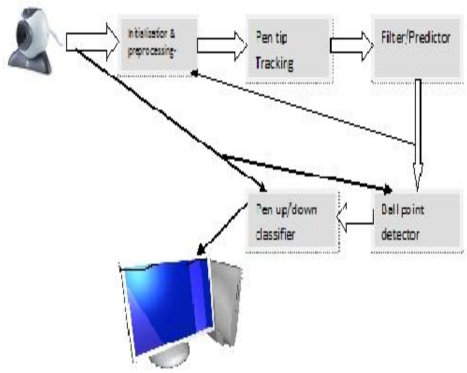

Figure 5: Block Diagram of the System

3.2 Initialization and Preprocessing

The first problem to be solved is to detect and locate the position of the pen tip in the first frame and to select the template to be used for detection in subsequent frames. There are two possible situations:

- The user writes with a pen that is familiar to the system.
- The user writes with a pen that unknown to system.

Figure 6 shows a sketch of the pen tip, which is seems to be roughly conical .Hence, the projection of pixels of the pen tip on to the image plane will be a triangle. Here, one of the borders of this triangle corresponds to the edge between the pen tip and the piece of paper. Detection and extraction of the pen tip template is reduced to finding the boundary points of the pen tip by computing the corresponding centroid and cutting a portion of the image around the centroid. The edges between the pen tip and the paper have bigger contrast than the edge between the pen tip and the finger. Thus, we only look for these two boundaries in the detection and extraction of the template for pen tip. There are some of methods to initialize the system when the pen is unknown. Here initialization method is a semi automatic one that requires a small amount of user cooperation.

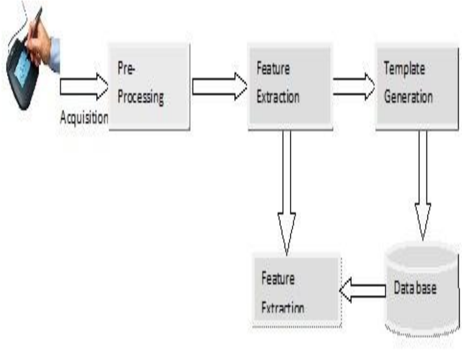

Figure 6: System Overview

4. ALGORITHM

In this algorithm depicts our camera-based online signature verification algorithm. There are two phases: an enrollment phase and a verification phase. In the enrollment phase, a user inputs his or her ID and writes several signatures for enrollment. During the writing process, images are captured by the web camera. Then, the pen tip position is tracked, and time-series pen position data are obtained. After preprocessing, several features are extracted, and the time-series data of the extracted features are enrolled as reference signatures and are also used for distance calculation. Then, a mean vector of each user is calculated and stored with the ID. In the verification phase, a user provides his or her ID and writes a signature (test signature). Images are captured, and time-series data of the pen tip position are obtained. After preprocessing, several features are extracted, and time series data of the extracted features are compared with the reference signatures to calculate several distances. Then, the calculated distances and the mean vector associated with the user ID are input to a fusion model, and a final score is computed. Based on this score, a decision is made. The enrollment and verification phases involve some of the following stages: (a) data acquisition, (b) pen tracking, (c) preprocessing, (d) feature extraction, (e) distance calculation, (f) mean vector calculation, (g) fusion, and (h) decision making. These stages are explained in this section.

4.1 Data Acquisition

A web camera for data acquisition is placed to the side of the writing hand, as depicted in Figure 3. In this figure, the web camera is placed on the left side of the writing hand because the writer is right-handed. The best position of the web camera for acquiring the online signature data is considered to be just below the writing surface. However, because the writing surface generally is not transparent, the pen tip position cannot be acquired from below the writing surface. Munich et al. set a camera above the surface [4]. In this position, the pen tip is sometimes covered by the hand, and therefore, users need to adjust the camera position in order that the pen tip can be acquired

4.2 Pen Tracking

The second module of the system has the task of tracking the position of the pen tip in the current frame of the sequence. The solution of this task is to get the optimal signal detection literature. Assuming that the signal to be detected is known exactly, the optimal detector is a matched filter which is a linear filter that looks like the signal one is trying to detect. In our case, the signal consists of the pixels that represent the pen tip and the noise has two components: one component is due to noise in the acquisition of the images and the other one is because of changes in the apparent size and orientation of the pen tip during the sequence of the images. The acquisition noise is the result of a combination of many factors like changes in illumination due to light flickering or automatic gain of the video camera, quantization noise, changes in gain of the frame grabber, etc. where not all these factors are effective. Changes in the apparent size and orientation of the pen while the user is writing significantly distort the image of the pen tip. The detection of the position of the pen tip is obtained by locating the maximum of the normalized correlation between the pen tip template and an image neighborhood centered on the predicted position of the pen tip.

Signature data was successfully obtained. The online signature data ***sig*** obtained from the images are:

$$\text{Sig} = (x_t, y_t)\ldots\ldots\ldots\ldots\ldots\ldots\ldots..\ (1)$$

$$t=1, 2\ldots\ldots.T.$$

Where T is the number of images. Note that only the pen position trajectories are available in camera-based online signature verification.

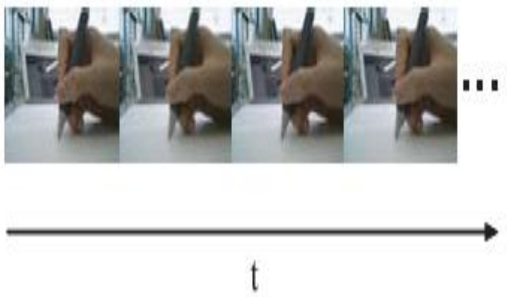

Figure 8: Acquired Image Data

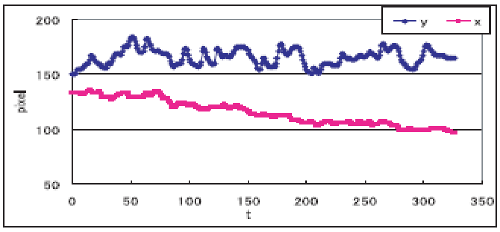

Figure 9: Pen position Tracking and Obtained Data

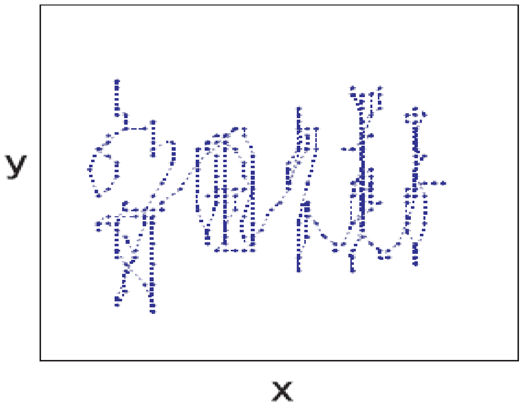

Figure 10: shape of an acquired signature

4.3 Preprocessing

The following transformation is performed to obtain the signature data:

$$\bar{x}_t = \frac{x_t - x_g}{x_{max} - x_{min}} \qquad (2)$$

$$\bar{y}_t = \frac{y_t - y_g}{y_{max} - y_{min}} \qquad (3)$$

Where

$$x_g = \frac{1}{T}\sum_{t=1}^{T} x_t \,,\; y_g = \frac{1}{T}\sum_{t=1}^{T} y_t$$

$$x_{min} = \min_t x_t \,,\quad x_{max} = \max_t x_t$$

$$y_{min} = \min_t y_t \quad,\quad y_{max} = \max_t y_t$$

4.4 Feature Extraction

The pen movement direction θ and the pen velocity |**V** | are calculated from the pen position data (x_t, y_t) as follows:

$$\theta_t = \tan^{-1}\frac{y_{t+1} - y_t}{x_{t+1} - x_t} \qquad \text{………………..} \ (4)$$

$$|V|_t = \sqrt{(x_{t+1} - x_t)^2} + \sqrt{(y_{t+1} - y_t)^2} \quad \text{…..}(5)$$

t = 1, 2... T-1

In the enrollment phase, M items of time-series data of the extracted features are enrolled as reference signatures.

Let the enrolled reference signatures ***Rsig***

Let the enrolled reference signatures $\boldsymbol{Rsig_m}$ be

$$Rsig_m = (rsig_{1,t}^{(m)} \,,\, rsig_{2,t}^{(m)})$$

$$= (\theta_t^{(m)}, |V|_t^{(m)}), \text{ ……………. } (6)$$

m=1, 2…... M

In the verification phase, the time-series data of the extracted feature ***Tsig*** is

$$Tsig = (t\;sig_{1,t} \,, t\;sig_{2,t})$$

$$= (\theta_t^{(0)}, |V|_t^{(0)}) \quad \text{………..………. } (7)$$

4.5 Distance Calculation

The distances between two sets of time-series data of the extracted features are calculated using dynamic time warping [11]. In the enrollment phase, the distances between reference signatures are calculated, and in the verification phase, extracted features from a test signature and reference signatures are calculated. A distance associated with θ and a distance associated with |**V** | are calculated independently. The calculated distance vectors in the enrollment phase are

$$D(Rsig_n \,,\, Rsig_m) \;= (D_1^{(n,m)} \,, D_2^{(n,m)}) \text{……… } (8)$$

$$= (dist_\theta^{(n,m)}, dist_{|V|}^{(n,m)}) \text{ … } (9)$$

n=1, 2, .M, m=1, 2……..M

Here, *D* (*Rsig*

Here, *D* ($Rsig_n$, $Rsig_m$) is a distance vector calculated between the *n*-th and *m*-th reference signatures, and the distance vectors calculated in the verification phase are

$$D\,(Tsig,\, Rsig_m) = (D_1^{(0,m)} \,, D_2^{(0,m)})$$

$$= (dist_\theta^{(0,m)}, dist_{|V|}^{(0,m)}) \quad \text{………. } (10)$$

m = 1, 2….M.

Where *D* (*Tsig*, $Rsig_m$) is a distance vector calculated between the time-series data of the extracted features and the *m*-th reference signature

4.6 Mean Vector Calculation

In the enrollment phase, a mean vector for each user is calculated as follows:

$$\text{Mean} = (\overline{D_1}, \overline{D_2}) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{(11)}$$

$$\bar{D}_i = \frac{1}{M(M-1)} \sum_{n=1\,m=1}^{M} \sum_{m \neq n}^{M} D_i^{(n,m)} \ \ldots \text{(12)}$$

And this mean vector is stored together with the user’s ID.

4.7 Score Calculation

A score for decision making is calculated in this stage. A distance vector and associated mean vector are input to a fusion model, and a final Score *is* computed:

$$\text{Score (Tsig)} = \frac{1}{M} \sum_{m=1}^{M} f(D(Tsig\ , Rsig_m\ ), \text{Mean}; \Theta)$$

Here, Θ is a parameter set of fusion model *f* (·). *L* simple perceptions are randomly generated, and these perceptions are combined using AdaBoost [13] to generate a fusion model. Thus, a parameter set is composed of weight parameters of simple perceptions and the confidence level of each perception.

4.8 Decision Making

A final decision is made based on the following rule:

$$\text{Tsig is} \begin{cases} Accepted\ if\ score(Tsig) \geq TRD(c) \\ Rejected\ if\ score(Tsig) < TRD(c) \end{cases}$$

Where *TRD*(*c*) is a threshold value and *c* is a parameter for adjusting the threshold value.

5. EXPECTED OUTCOME

The expected outcome depended on the fact that the setting of threshold. When feature was taken into consideration for verification, left hand cam was the best. This observation is easy, because feature ix in the images from left hand cam is much consistent with the y-coordinate information in real space, whereas feature in the images from front hand cam is consistent with the x-coordinate information in real space. Equal Error Rate (EER) tradeoff curves for left hand camera the evaluation of each feature using the equal error rate (EER) computed as the intersection of the false acceptance rate (FAR) and the false rejection rate (FRR) curves. FAR (False Acceptance Ratio): A false identity claim is accepted. FRR (False Rejection Ratio): The error rate that a true user identity claims is falsely rejected. We computed EER of each feature individually to evaluate the accuracy of each feature.

6. ACKNOWLEDGEMENTS

The authors would like to thank everyone, whoever remained a great source of help and inspirations in this humble presentation. The authors would like to thank K.L. University management for providing necessary facilities to carry out this work.

7. REFERENCES

[1] Muhammad Nauman Sajid “Vital Sign: Personal Signature based Biometric Authentication System”, Bs degree thesis, Pakistan Institute of Engineering and Applied sciences, Sep 2009.

[2] R. S. Kashi , J. Hu & W. L. Nelson, “On-line Handwritten Signature Verification using Hidden Markov Model Features”, Fourth International Conference Document Analysis and Recognition (ICDAR'97), pp. 253 – 257, 1997.

[3] Charles E. Pippin, “Dynamic Signature Verification using Local and Global Features”, Georgia Institute of Technology, July 2004.

[4] Hao Feng and Chan Choong Wah, “Online Signature Verification Using New Extreme Points Warping Technique”, *Pattern Recognition Letters*, vol. 24, pp. 2943-2951, Dec. 2003.

[5] F.A. Afsar, M. Arif and U. Farrukh, “Wavelet Transform Based Global Features for Online Signature Recognition”, Proceeding of IEEE International Multi-topic Conference INMIC, pp. 1-6 Dec. 2005.

[6] Liang Wan, Bin Wan, Zhou-Chen Lin “On-Line Signature Verification with Two-Stage Statistical Models”, Eighth International Conference on Document Analysis and Recognition (ICDAR'05), pp. 282 – 286, 2005.

[7] Alisher Kholmatov, “Biometric Authentication Using Online Signatures”, MS Thesis, Sabanci University, June 2002.

[8] Chan F. Lam, David Kamins and Kuno Zimerann, “Signature Recognition through Spectral Analysis”, Pattern Recognition, vol. 22, pp.39-44, Jan.1989.

[9] Mario Enrique Munich “Visual Input for Pen-Based Computers” PhD thesis, California Institute of technology, Pasadena, California.

AUTHORS PROFILE

T.Venkatesh, presently pursuing M.Tech Degree in Department of Electronics and Computer Engineering in Koneru Lakshmaiah University.

S. Balaji, Currently working as HOD & Professor in Dept. of Electronics and Computer Engineering in Koneru Lakshmaiah University, Guntur. He has published 21 Papers in various International journals and conferences. His Research Areas are Biometrics, Security and Image Processing.

Dr. A. S .N. Chakravarthy, Currently working as Professor in Dept. of Electronics and Computer Engineering in K.L. University, Guntur. He has 14 papers published in various International journals and conferences. His research areas include Cryptography, Biometrics, and, Digital Forensics. He is Reviewer & Editorial Board Member for Various International Journals.